N65 88457

Code None

23p

RELIABILITY ANALYSIS FOR SPACE SYSTEMS [redacted] 1

William W. Wolman * [1963] 23p ref [redacted]

National Aeronautics and Space Administration

Goddard Space Flight Center, Greenbelt, Md.

(NASA TMX-54624)

Introduction

On October 4, 1957, the Soviet Union launched the first man-made satellite, Sputnik I, into orbit. On January 31, 1958, the United States launched its first satellite, Explorer I. This marked the beginning of the Age of Space, and the reliability of space systems became a well defined major problem for the scientist and engineer.

The word reliability as used in this talk refers to the probability that a system, subsystem, component or part will perform its required functions under defined conditions at a designated time and for a specified operating period. By probability we refer to a quantitative measure or to the likelihood of dependable operation. A space system consists of a launch vehicle, spacecraft and ground support equipment used in launching, operating and maintaining a vehicle or craft in space.

a Conf.

It makes sense to consider reliability as a <u>systems</u> parameter, or even more general as a basic requirement for a mission. For example, one of Goddard's programs consists of

* Presented at the 23rd National Meeting of the Operations Research Society of America ~~on May 28, 1968 in~~ Cleveland, ~~Ohio~~ 28 May 1963

Unc [redacted]

[redacted]

the development of a meteorological satellite system, namely the Tiros project. It would indeed be a folly to concentrate only on the spacecraft TV camera system, rather than the entire space system consisting of the Delta launch vehicle, the Satellite and the ground station complex. The reason being that a system is only as reliable as its weakest constituent element or subsystem. Maintenance and repair in flight, no matter how trivial, is not possible at this time, especially for unmanned systems. It requires a balanced effort in terms of resources and such factors as the state-of-art, schedule, cost and experience to achieve a desired level of reliability.

Historically, we can attribute the growth and evolution of the reliability disciplines, the major areas being in the engineering and mathematical-statistical fields, to the development of complex electronic systems during and after World War II. And later, the emergence of the guided missile as a weapons system, resulted in new reliability problems reaching their pinnacle with ICBM systems. Those of us who have been concerned with reliability problems of space systems realized fairly soon that many of the problems and approaches required are similar to those for the missile systems - however, there are certain distinct conceptual differences which require new and different approaches. Let me enumerate some of these differences:

(1) The main purpose of a missile system is to inactivate a military objective within given tactical restraints.

It may be possible to achieve this with 40 missiles each having a reliability of .30, or 20 each with a reliability of .60 or even 12 each with a reliability of 1. In each case we would have the same expected number of successes. In actuality the problem is considerable more complicated since such factors as miss distances and operating times must certainly also be considered.

(2) In the development of a space system we are concerned with a specific scientific objective, for example, the launching of an astronomical observatory with a large telescope, putting a man into orbit for a day to perform experiments, or making radiation measurements in a 70,000 mile eccentric orbit. A complete program may consist of 3 to 5 flights, even to assure at least two successes in, say, 4 trials with a probability of .95 requires a <u>single</u> trial probability of success of about .75. Or if at least 2 successes are required with probability of .99 then the single trial probability of success has to be .85.

(3) In the exploration of space we are still almost exclusively concerned with research and development efforts. There is no such thing as a production run at a systems level.

I am <u>not</u> saying that military programs do not require and desire high reliability, but that NASA in its programs must have a very high <u>single</u> trial probability of flight success in order to achieve its objectives and this is required for the very first flight. The manned space flight programs are perhaps the most dramatic examples of this, although for the launching of a 10 to 20 million dollar scientific observatory, an analogous argument can be made. In summary, it can be stated that for space systems there is no acceptable trade-off between the number of systems available to meet the objective and reliability. Redundancy at the over-all space systems level is not an acceptable means of achieving reliability due to safety, cost and time considerations.

Manned and Unmanned Systems

In considering reliability problems for space systems, I shall make the somewhat arbitrary division between manned and unmanned systems. The reasons for this will become apparent as the discussion is developed. One of the major differences between manned and unmanned systems is that for manned systems, safety is an overriding requirement, and this involves a complete technology for the life support systems as well as the integration of man into the system.

Manned Space Systems

The manned space programs of the National Aeronautics and Space Administration are projects Mercury, Gemini and

Apollo. My remarks concern only project Mercury, however, at least conceptually, some of the ideas concerning reliability carry over to Gemini and Apollo. The following comments on project Mercury pertain to a reliability analysis with which I was involved in from 1960 to 1962. It is discussed in more detail in reference (1).

A Mercury reliability study was initiated in June of 1960 by the National Aeronautics and Space Administration in Washington, D. C. Its purpose was to provide overall estimates of reliability for the Mercury capsule and booster system for both the unmanned and manned missions as defined below. In addition, it was desired to highlight the areas of unreliability that existed in the system.

This study was divided into two phases: the unmanned mission and the manned mission. The unmanned mission was considered to be that which would be required of the Mercury capsule with the assumption that no astronaut was aboard but that the life support systems were required to function. The manned mission, on the other hand, assumed that the astronaut was aboard the capsule and that he could function as required.

(1) NASA Technical Note TND 1558, "A Reliability Model And Analysis For Project Mercury - 3-Orbit Manned And Unmanned Mission," by William Wolman and Fred Okano, National Aeronautics and Space Administration, Washington, D.C., December 1962.

The normal mission is defined as a 3-orbit mission from capsule umbilical drop to touchdown, while flight safety is defined as the successful completion of the normal mission or of any of the aborts possible at various times of the normal mission. An abort is defined as the necessity, due to some failure, to terminate the normal mission and bring the capsule to earth prematurely.

In order to complete this study, a number of assumptions were necessary. These assumptions were:

1. The cut-off date for the system and test data, as used in this study, was July 1, 1960. Since that date, additional testing had been performed and there had been some changes in the design of the system as well as changes in the mission ground rules.

2. The system considered consists only of the capsule from the period of capsule umbilical drop to touchdown and the Atlas booster (including Abort Sensing and Implementation System). The study goes up to time of touchdown and does not include any aspect of the recovery operation. For example, the equipment necessary in the capsule itself, such as d-c power, which may be required in locating the capsule by recovery forces, is assumed to have to function only up to time of touchdown.

3. No failures are due to:

a. Capsule structure
b. Abort Sensing and Implementation System
c. Ground support systems

4. All subsystems and equipments are functioning perfectly at time of umbilical drop. That is, effective check-out procedures have eliminated all malfunctions present in the system and, moreover, no failures occur between check-out and umbilical drop.

5. The test program for all subsystems and components duplicates the actual environmental stresses of the mission. It is known that the environmental stresses cannot be completely duplicated; however, it had been assumed that the reliability of the subsystems is that which had been demonstrated by the various test programs.

6. The mathematical and statistical models used truly describe the mission. These models are discussed further in the following section.

7. If all subsystems function as designed, then the normal mission and safety reliabilities will be one. Failures will occur only in the equipments which do not function as intended.

8. Quality control failures are not involved in malfunctions. This means that contractor receiving, assembly, and check-out inspections will effectively identify all areas of malfunction. The failures that have been included in estimating the subsystem reliabilities are those that could occur during the mission.

A failure, for example, which would result from a diode put in backwards should be detected during some phase of inspection and would therefore not be included. Also, failures that may occur at random are included since they may or may not be identified during inspection (whether or not corrective action has later been taken).

9. In those instances where the estimates of subsystems reliability is based on very sparse data, the subsystem is assumed to have passed the acceptance criteria.

10. As opposed to hardware, which, once it has failed cannot be repaired, the astronaut, if unable to perform at one time, can recover and perform his required functions in succeeding time periods.

11. Aborts from orbit are initiated at the end of orbit. Unless a catastrophic failure occurs, such as rapid oxygen depletion, this is actually the case in order to maximize the probability of recovery after touchdown.

12. Except for the d-c and a-c Power Supply Systems and the systems specifically noted, all major systems listed below, comprising the overall Mercury system, are considered to be functionally and stochastically independent of each other for purposes of this study.

a. Booster

b. d-c Power System

c. a-c Power System

d. Environmental Control System

e. Telemetry

f. Attitude Control and Stabilization System (ASCS) including retrograde initiation and retro-rocket firing *

g. Communications System

h. Capsule Tracking System, including C and S Band Beacons and Command Receivers

i. Tower Ring Separation

j. Escape Rocket Firing

k. Capsule Ring Separation

l. Posigrade Rocket Firing

m. Periscope Extension

n. Retrograde Package Jettison

o. Periscope Retraction

q. Antenna Fairing Ejection

r. Main Chute Deploy

s. Landing Bag Extension

13. Both the telemetry and the communications systems are required during the mission.

* Includes Communications, Telemetry, and Capsule Tracking Systems during retrograde initiation and retro-rocket firing.

14. The astronaut is not required to orient the capsule during orbit at night in case of ASCS failure. However, he is required to perform this maneuver in daylight, including retrograde maneuver.

The times of initiation and completion of the normal unmanned mission, as well as the eight aborts, are shown in Fig. 1. The times for the manned mission are identical except that the unmanned abort C (tower-separation circuit failure) does not exist for the manned mission since the crew override which initiates this abort is the same override required to continue the normal mission.

The "overall" reliability diagram is shown in Fig. 2. The overall diagram depicts the systems that must operate, in their relative sequence, in order for the mission to continue or for an abort to succeed. The systems have been given "link" numbers" for identification purposes. For example, link 1 is the booster operating from capsule umbilical drop to 8-inch lift-off; link 2 is the booster from lift-off to escape tower jettison. The aborts have been identified by having upper case letters corresponding to the abort (A through G) follow the link number.

The fundamental probability model for the analysis can be described by the following equation:

$$\Pr\ \{\text{Flight Safety}\} = \Pr\ \{\text{Successful 3-orbit normal mission}\} + \Sigma \Pr\ \{\text{Need to abort and abort successfully}\}$$

where we define the letters "Pr" to mean "the probability of" and the summation on the right hand side of the above equation is extended over all possible mutually exclusive aborts.

We can then express the above equation as follows:

$$\Pr\ \{\text{Flight Safety}\} = \Pr(S_k) + \Sigma \Pr\ \{M_{i-1}\ \overline{M}_a\ m_a\ m_{1_j}\}$$

where,

S_k is event: Successful 3-orbit mission from lift-off to touchdown

M_{i-1} is event: normal mission to time t_{i-1}

$\overline{M}_a$ is event : failure of normal mission some time prior to t_a.

m_a is event : able to abort

m_{1_j} is event : abort successfully through time of touchdown

and

the j - th abort (j is one of the aborts A through G2) is divided into time periods

$$0 = t_o < t_1 < t_2 < \cdots < t_{i-1} < t_a < t_i < \cdots < t_{1_j}$$

The problem of estimating the parameters of the above model was a severe one in terms of complexity and volume of test data which had to be processed. It was achieved with the assistance of electronic computing equipment. Table I shows the outline of the final form which some of the outputs of the analysis resulted in.

In summary, the model and methods used are in many ways idealizations of true system operation and the approach taken, namely, estimating overall system reliability on the basis of information on subsystems, components and parts, has its shortcomings. However, there exists at present no other means of assessing the reliability of a highly complex system using a rational approach and a quantitative basis, than by using an approach, at least similar in concept, to that used for the Mercury analysis described briefly above.

Although the model was developed for the evaluation of the Project Mercury 3-orbit mission, the approach is general and can be modified for other space system applications.

Unmanned Space Systems

One of the Goddard Space Flight Center's major responsibilities is the management, including the development, production and testing of unmanned satellites to be launched into the cislunar space. This may involve a communications satellite system such as Relay or an Orbiting Astronomical

Observatory (OAO) which will enable us to launch a 38 inch telescope into space.

In the exploration of space we encounter the broad problems found in any science, namely we are concerned with systematized knowledge based on <u>observation</u> and <u>experimentation</u> in order to determine the underlying principles of what is being studied. We are led to one of the prime objectives of any scientific approach, namely the desire to be quantitative and numerical. The power and usefulness of numerical measures are that they provide a more precise description and framework of the area under study. A few examples of reliability and related problems in unmanned space applications in this area are:

(a) What are the trajectory errors involved in injecting a spacecraft into orbit? This is the key launch vehicle problem, namely to be at the right place with the right velocity.

(b) What is the exact pattern over time of the enhanced radiation belt. This is vital information for manned space flight. And, what is the effect of radiation on a spacecraft or satellite system?

(c) What is the capacity of the data and communication handling system for the Orbiting Geophysical Observatory with a capacity of 20 to 50 experiments launched in polar or eccentric orbit?

(d) What are the electro-magnetic radiations from the sun as measured by the Orbiting Solar Observatory?

(e) What is the reliability of the Atlas/Agena launch vehicle?

(f) How do we measure the particles traveling in space? Namely, the meteoroid hazard.

The field of reliability analysis as a scientific and technological area concerns itself with problems not much different from many other disciplines. It is involved with the question of quantifying or measuring and the desire and ability to predict the future. Furthermore, it is an objective to establish quantitatively cause and effect relationships for the functioning of the space systems involved.

Reliability analysis is the area in which I have been personally involved in to a considerable extent in NASA. To say that reliability analysis is solely a statistical and probabilistic problem is just as meaningless as it is to say that Newton's laws of physics or Kepler's laws governing the movement of planets are part of a purely mathematical discipline. However, I will say that the cornerstone <u>for</u> the assessment, evaluation and understanding, of reliability, considered as a design parameter, depends on stochastic phenomina; and these can only be described adequately in statistical and probabilistic terms.

Apparently, we are not the only ones who have this point of view. Let me quote for you:

"The criterion of reliability of a complex technological component depends on an aggregate of interconnected factors, the chance quantities, and is a typical statistical parameter. All measures taken to raise reliability should therefore be based foremost on statistical analysis of the influencing factors at all stages of development - in production, in transport, storage and in utilization of the components", from an article entitled "The Science of Reliability", USSR translation, written by Academician A. Berg in Ekonomischeshoya, Gazetal No. 184, Moscow, 8 June 1961.

Furthermore, Berg states:

"On the basis of mathematical statistics and the mathematical theory of probability the beginnings of a mathematical theory of reliability have already made their appearance. There is an extensive Soviet and foreign literature covering this problem."

The quotations are self explanatory.

If I had to select the single most difficult reliability analysis or perhaps operations research type problem in the space program I think it would be not much different than that for problems in many other scientific areas, physical or social namely, to determine "What are the precisely defined problems"? Consider the area of measuring reliability. How do we establish or determine the design goals for the reliability of a space system". Do we - as has and is being done - specify a number, say .80 and say this is to be the probability or reliability that our system shall function for one year, say, our proposed Orbiting Observatories. I think a little reflection will show that such factors as the program objectives must be taken into account separately for the following two types of satellite systems:

(a) Scientific Satellites

This category includes such systems as the Orbiting Astronomical Observatory and the Orbiting Geophysical Observatory. This later system is capable of providing up to 50 different experiments in one flight for short and long term geophysical studies.

(b) Applications Satellites

This category includes such meteorological satellite systems as Nimbus to continuously provide weather data for all parts of the earth and communications satellite systems such as Relay and Syncom.

For scientific satellites we may wish to specify different reliability requirements for different experiments since some experiments may require only 30 days of operation whereas others may require a whole year of observation. Furthermore, rather than measuring reliability in terms of probability of success for a period of time, it is often more meaningful to require that a certain percentage of information is to be transmitted successfully.

The reliability measures for applications satellite systems should be related to the functional requirements of the system. By this I mean for example in the case of a meteorological satellite, we are interested in having say 75% of all cloud pictures transmitted daily to be acceptable and we require this for at least 90 days. Or for a communications satellite we may define reliability as the number of hours of satisfactory communications coverage at specified band width.

The classical reliability measure of probability of success would still be applied to such areas as launch vehicle reliability. It makes sense to speak of a 95% reliable launch vehicle, namely on the average 19 out of 20 launches with a specific vehicle would result in successful insertion of the spacecraft into orbit.

Questions in the assessment of reliability involve all the problems of estimation and the complex question of how to find confidence intervals for intricate mathematical functions. The question of how to develop estimates on the basis of a test program is another much discussed and difficult problem. Questions which must be answered involve the problem of the underlying distribution. Most of the time the exponential and more generally the Weibull distribution are being used. Non-parametric theory is needed.

Another specific reliability problem involves the growth of reliability over the development period of a system and how to measure this empirical and observed phenomia. In the space program, we desire to minimize or as stated previously to eliminate reliability growth - reliability must be at its maximum with the first experiment for the reasons of safety, time and cost.

Summary

I have discussed briefly several aspects of reliability analysis for manned and unmanned space systems. It should be realized that reliability analysis is only one aspect of the overall area of reliability. We at the Goddard Space Flight Center consider the major elements of a reliability program to consist of the following:

(a) Reliability Assessment - The procedure which provides probability estimates of the system, subsystem and components at appropriate steps of design, development and assembly in order to evaluate the likelihood of meeting established reliability goals.

(b) Quality Assurance - The effort to make certain that materials and supplies manufactured and produced under applicable Specifications are in accord with the intent of design and are of a satisfactory level of quality.

(c) Environmental Tests - The systems tests performed on the ground which simulate all significant stress conditions imposed on the spacecraft during handling transportation, launch and space flight or operational use.

In closing I would like to remark that reliability problems can be considered from an operations research viewpoint. We have an inter-disciplinary subject which requires a team effort. We do have quantitative and probabilistic models, we require a rational approach based on facts and past experience. And last but not least we certainly have a function to maximize - namely the reliability.

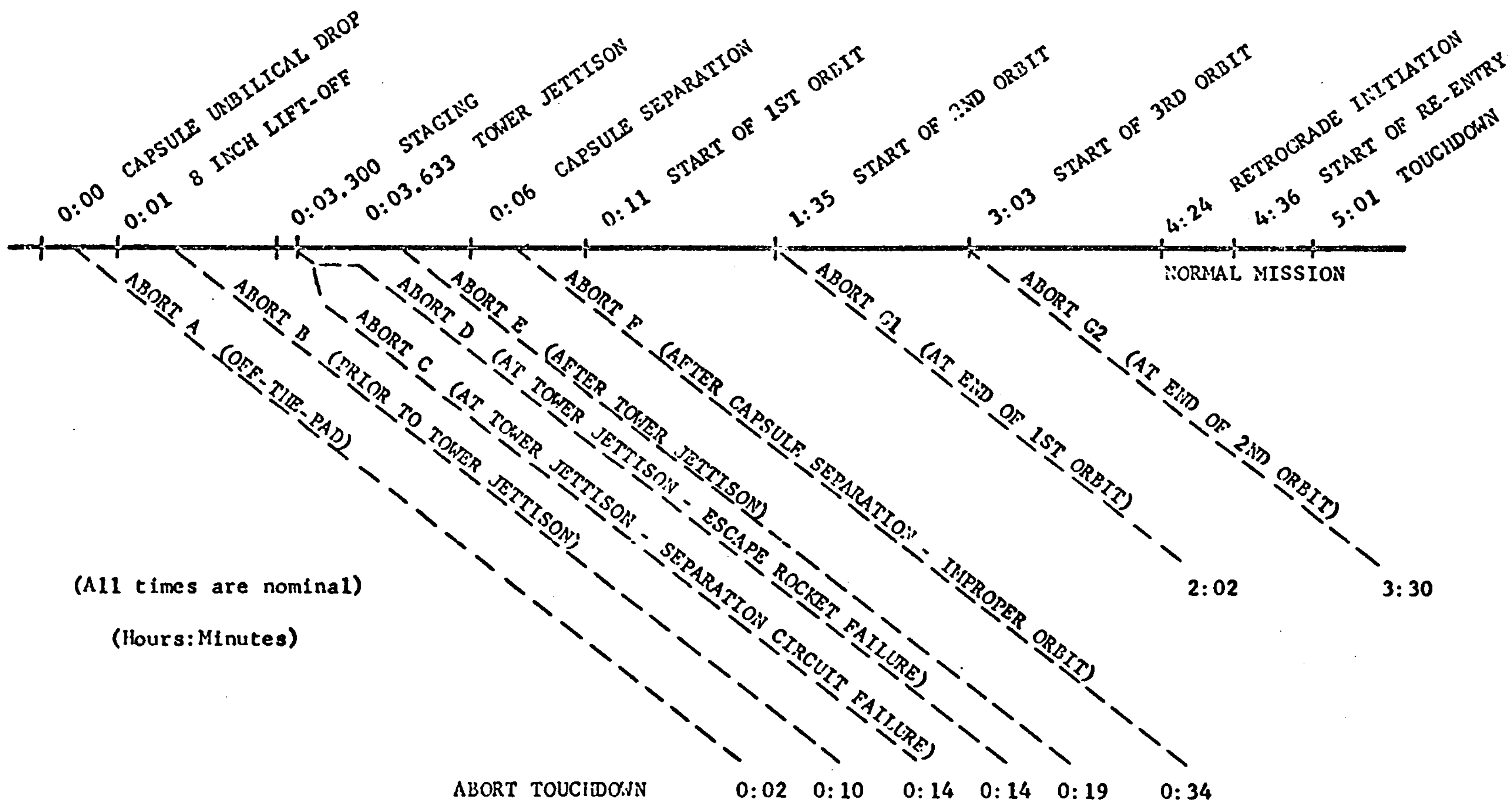
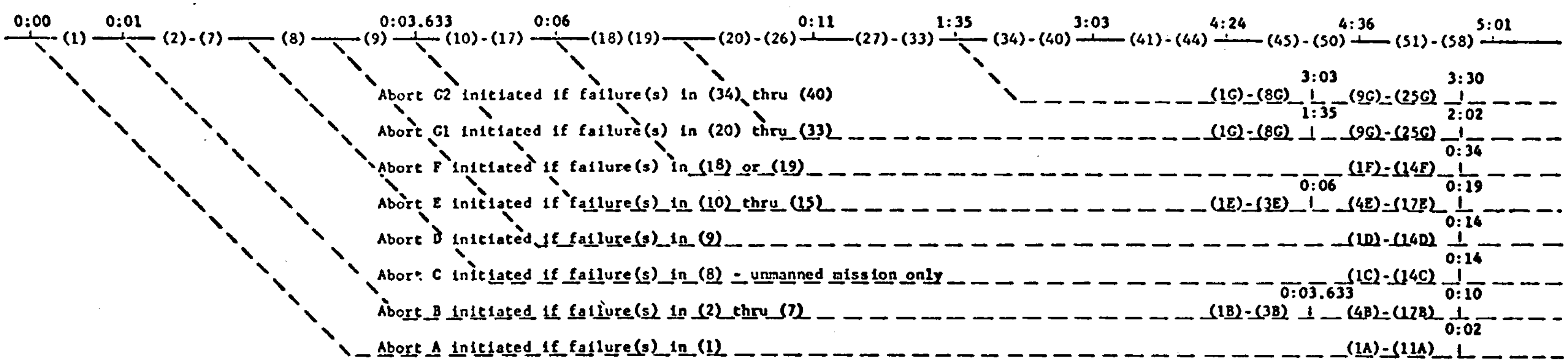


Fig. 1 TIME SCHEDULE OF NORMAL MISSION AND ABORTS FOR PROJECT MERCURY



System	Link Number	System	Link Number
Booster	(1), (2), (10), (18)	Tower Ring Separation	(8), (7A), (11B), (8C)
D. C. Power Supply	(3), (11), (20), (27), (34), (41), (45), (51), (1A), (1B), (4B), (1C), (1D), (1E), (4E), (1F), (1G), (5G), (9G), (17G)	Escape Rocket Firing Capsule Ring Separation Posigrade Rocket Firing	(9), (5A), (9B), (6C), (6D) (16), (4A), (8B), (5C), (5D), (8E) (17), (7D), (9E)
A. C. Power Supply	(4), (12), (21), (28), (35), (42), (46), (52), (2A), (2B), (5B), (2C), (2D), (2E), (5E), (2F) (2G), (6G), (10G), (18G)	Capsule Tracking Communications Periscope Extension	(19), (32), (39) (24), (30), (37) (25)
Environmental Control System	(5), (13), (22), (29), (36), (43), (47), (53), (3B), (6B), (3C), (3D), (3E), (6E), (3F), (3G), (7G), (11G), (19G)	Retro Package Jettison Periscope Retraction	(49), (6A), (10B), (7C), (8D), (13E), (7F), (15G) (50), (15E), (9F), (16G)
Telemetry	(6), (14), (23), (31), (38)	Drogue Chute Deploy	(55), (14B), (11C), (11D), (17E), (11F), (22G)
Attitude Control System, incl. Retro Rocket Firing	(7), (15), (26), (33), (40), (44), (48), (54), (13B), (10C), (9D), (10D), (10E), (11E), (12E), (14B), (16E), (4F), (5F), (6F), (8F), (10F) (5G), (6G), (12G), (13G), (14G), (20G), (21G)	Antenna Fairing Ejection Main Chute Deploy	(56), (9A), (15B), (12C), (12D), (18E), (12F), (23G) (57), (10A), (16B), (12C), (13D), (19E), (13F), (24G)
Abort Initiation	(3A), (7B), (4C), (4D), (7E)	Landing Bag Extension	(58), (11A), (17B), (13C), (14D), (20E), (14F), (25G)

Fig. 2 OVERALL RELIABILITY DIAGRAM FOR THREE-ORBIT MERCURY MISSION
(Link numbers are shown in parentheses)

Table 1

PROBABILITIES OF MISSION SUCCESS AND FLIGHT SAFETY

	Probability of										
Time period	I Success up to beginning of period (U*)	II Success through end of period (U*)	III Abort being required (U-J*)	IV Being able to abort		V Successful abort		VI Abort failure		VII Being unable to abort	
				A (C*)	B (U-J*)	A (C*)	B (U-J*)	A (C*)	B (U-J*)	A (C*)	B (U-J*)
		**									
									Σ(VI-B)		Σ(VII-B)

$1 - [\Sigma(\text{VI-B}) + \Sigma(\text{VII-B})] = Pr\{\text{Flight Safety}\}$

*U: unconditional; U-J: unconditional-joint; C: conditional

**Mission success